REMARKS

This Amendment is being filed in response to the Office Action dated May 6, 2004. Reconsideration and allowance of the application in view of the amendments made above and the remarks to follow are respectfully requested.

Claims 1-12 are pending in this application. Claims 1 and 9-11 are independent claims.

In the Office Action, Claim 3 and 8 are indicated as allowable if amended to be in independent form including all of the limitations of the base and intervening claims. The Applicant thanks the Examiner for this indication.

The specification is objected to for failing to reference FIG. 4 on page 9, line 28. The specification is amended herein in accordance with the Examiner's suggestion. Accordingly, it is respectfully submitted that the specification is in proper form and an indication to that effect is respectfully requested.

The drawings are objected to for failing to comply with 37 C.F.R. 1.84(p)(4) because it is stated, in effect, that reference character 232 is used to designate KCB_N and KBC_{N+1}. This rejection of the drawings is respectfully traversed. MPEP 608.02(e) makes clear that "no single reference character [should be] used for two different parts or for a given part and a modification of such part..." However, in this case it is respectfully submitted that reference character 232 is utilized to depict only a single object

in both of FIGs. 2, and FIG. 5, specifically "key check block (KCB) sub-field 232" as described in the paragraph starting at page 6, line 16, particularly at page 7, lines 2-9 with regard to FIG. 2. A further description with regard to FIG. 5 is contained at page 10, lines 6-7 wherein it is stated that (emphasis provided) "[t]he key check **block KCB_N in field 232** of packet 500 is used to verify which key was used to encrypt packet 500." Further at page 10, lines 14-16 it is stated that (emphasis provided) "packet 510 includes the reference key check block KCB_{N+1} **in the key check block sub-field 232**, but now encrypted with the source session key used for this packet ..."

Accordingly, as should be clear, reference character 232 is used to designate the field (key check block sub-field) and not the identity of the key check block contained therein, whether it be key check block KCB_N, key check block KCB_{N+1}, or otherwise. This field is the same in each place designated and therefore it is properly identified in each place. It is common and proper that the same designation may be used in different figures for designating the same object (in this case field) so it is respectfully submitted that this objection to the figures is improper and an indication to that effect is respectfully requested.

Claims 1, 2, 4-7, and 9-12 are rejected under 35 U.S.C. §103(a) as unpatentable over U.S. Patent No. 6,223,285 to Komuro

("Komuro") in further view of U.S. Patent No. 5,706,348 to Gray ("Gray").

Komuro shows a method and system for transferring information using an encryption mode indicator (EMI) 210 located in the header portion 240 of an information packet 200 (see Komuro, FIG. 4, and the accompanying description contained in Col. 6, lines 61-65). The EMI indicates the copy protection attributed to the information packet and also the type of encryption used in the information packet (e.g., see Komuro, Col. 7, lines 1-5). In the shown embodiments, circuits 440 and 540 are utilized by the respective receivers shown in FIGs. 5A and 5B to extract the header information from the information packet and extract the EMI (see, Col. 8, lines 16-18 and Col. 10, lines 6-11).

Now while it is true that the EMI indicates the type of encryption utilized by the data packet, it does so merely by the value of the EMI (see, TABLE I and accompanying description contained in Col. 6, lines 18-34) and is not identified by the receiver based on a valid decryption of the EMI. In fact, Komuro teaches (emphasis provided) "that while the present [Komuro] invention encrypts the data portion 22 of packet 200 (if in EMI mode A or EMI mode B), the header sections 230 and 240 remain unencrypted when transmitted ..." and it is in the header section 240 wherein the EMI is contained (See, Komuro, FIG. 4 and Col. 7,

lines 5-9.) Accordingly, the EMI is transmitted in an unencrypted state.

Accordingly, Komuro does not disclose or suggest a (emphasis provided) "source device including: ... an encryptor for encrypting at least part of the data field of a packet under control of the active source session key; the encrypted part of the data field including a sub-field designated as a key check block field; the sink device including: a key generator for generating a plurality of candidate sink session key in a predetermined sequence of sink session keys Ksinki, where for each index i in the sequence the respective sink session key Ksinki corresponds to the respective source session key Ksourcei; a decryptor for decrypting at least part of the data field of a received packet under control of a sink session key; a key resolver operative to determine which of the candidate sink session keys corresponds to the source session key used to encrypt the encrypted part of a received packet, by causing the decryptor to decrypt the data in the key check block field of the received packet under control of each time a different one of the plurality of candidate sink session keys **until a valid decryption result is found**; and to cause the decryptor to decrypt a remaining encrypted part of the data field of the packet under control of the candidate sink session key which produced the valid

decryption result" as required by Claim 1. In fact, as discussed above, Komuro teaches transmitting the EMI in an unencrypted form.

Gray is a system for changing session keys that are utilized in an encryption/decryption process. As described in the summary of the invention of Gray, the Gray system provides 9emphasis provided) "a simple technique for maintaining synchronization between the key used in encrypting the data packet at a source node in a data communication network and the key used in decrypting the same data packet once it is received at a destination node in the network... before a new key can be activated at a destination node, the key necessarily must have been communicated to that node... When the source node decides to activate the new key, it transmits a marker packet having a unique format. The source node then begins encrypting data packets using the new key. When the destination node recognizes the marker packet, it discards the marker packet and activates the new key to decrypt subsequently-received data packets." (See, e.g., Gray, Col. 2, line 54 through Col. 3, line 2., also Col. 5, lines 7-10, 14-22, 61-64, and Col. 6, lines 8-27.)

Accordingly, the updated keys of Gray are periodically transmitted from the transmitter to the receiver. Gray does not disclose or suggest that the keys are in a predetermined sequence. Gray further shows using a marker packet, encrypted using a current

key to indicate to the receiver that a new key will be subsequently utilized by the transmitter. The marker packet is compared to a value corresponding to the current key and new key (which is previously received at the receiver) to determine that it is a valid marker key (see, Col. 6, lines 19-27), thereby indicating that the receiver should start decrypting subsequent data packets utilizing the new key.

Gray is cited for showing "generating session keys in a predetermined sequence ... Col. 2, lines 35-36 of Gray is cited for this feature (see, the Office Action, page 4, first paragraph). However, in fact, Gray in this section merely recites "periodically chang[ing] the keys used for encryption/decryption" (see, the cited section and the above discussion) which does not disclose or suggest that the keys be changed in a "predetermined sequence" as required by each of Claims 1 and 9-12.

Gray is also cited for showing (emphasis provided) "causing the decryptor to decrypt the data in the key check block field of the received packet under control of each time a different one of the plurality of candidate sink session keys until a valid decryption result is found" (see, the Office Action, page 4, lines 4-6). In fact, Gray teaches that the marker indicating to the receiver to subsequently start using the new key is transmitted from the transmitter to the receiver using the current encryption

key (see, discussion above and Col. 5, line 22 of Gray). The new key is only activated after the marker packet is identified (see, the discussion above and Col. 6, lines 28-35 of Gray) by recurrently decrypting the marker field of separate data packets utilizing the same (current) key until a valid marker is identified.

Accordingly, Gray does nothing to cure the deficiencies in Komuro. Since the this element is required by each of Claims 1 and 9-12, it is respectfully submitted that each of Claims 1 and 9-12 are allowable over Komuro in view of Gray for this and the other above reasons and an indication to that effect is respectfully requested.

Claims 2-8 depend from Claim 1 and accordingly are allowable for at least this reason as well as for the separately patentable elements contained therein. Accordingly separate consideration and allowance of each of Claims 2-8 is also respectfully requested.

Based on the foregoing, the Applicant respectfully submits that Claims 1-12 are patentable over the cited prior art, and notice to this effect is earnestly solicited.

Applicants have made a diligent and sincere effort to place this application in condition for immediate allowance and notice to this effect is earnestly solicited.

Early and favorable action is earnestly solicited.

Respectfully submitted,

By _____

Gregory L. Thorne, Reg. 39,398
Senior Patent Counsel
(914) 333-9665
September 7, 2004

CERTIFICATE OF MAILING

It is hereby certified that this correspondence is being deposited with the United States Postal Service as first-class mail in an envelope addressed to:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

On 09/07/2004

By _____
Mailing Party